Compliance Documentation

Document prepared by the CloudShield team

Frederico Rosa

Gonçalo Afonso

Tatiana Meneses

Tiago Duarte

Table of Contents

1. What is GDPR?

General Data Protection Regulation (GDPR) is an international framework that lists a large number of privacy and security law requirements that organizations all around the world should implement. These laws are meant to be applied in any collection of data processes related to people within the EU, specifically:

- personal data (PII - Personally Identifiable Information - and PCI - Payment Card Industry);
- data processing;
- data subject;
- data controller;
- data processor.

"With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence" (https://gdpr.eu/what-is-gdpr/).

To improve companies security and confirm that they were enforcing these guidelines, a supervisory authority (the Information Commissioner's Office - ICO) was established. Its goal was to encourage and advise the implementation of the GDPR legislation and apply accountability when needed. For the field of cybersecurity, the guidelines require that personal and critical data should be processed and collected securely, by using appropriate techniques. For this purpose, a GDPR Security Outcomes was developed.

This framework outlines a set of outcomes that companies and organizations should process in order to achieve their goal, such as:

- manage security risks;
- protect personal data;
- detect security events;
- minimize (and mitigate) attacks and impact.

The GDPR official website sets as a crucial guidance for companies to be able to implement all of these measures. It provides numerous documentation that can help with the achievement of maximum security.

Another important measure to be applied is an incident report plan. “If you are affected by an incident which involves (or is likely to involve) a breach of personal data, then you are likely to have an obligation under the GDPR to notify the ICO” (https://www.ncsc.gov.uk/information/gdpr). More information about the stages can be found in the ICO official website.

Security incidents are increasingly taking a strong negative impact, not only on companies and organizations, but national and international wide. For this particular reason, it became crucial to report any potential (inter)national incidents that might have such an impact. Which is why it is important to seek ICO’s guidance and support to constraint the possible breach. If, on the other hand, there is a possible event that doesn't have a national impact, it should be reported to the Action Fraud center, located in the UK.

2. GDPR encryption policy

Nowadays, it has become a normal procedure to collect personal data from the population. However, this process is associated with a high level of risk. It is now possible for companies to reduce the probability of data breach or even stolen data, by implementing encryption policies. With this measure, information is converted into a secret code that can only be unlocked with a unique digital key.

GDPR sets multiple articles regarding the process of personal data and attribute accountability, when it needs to be applied. Article 32 of the GDPR, “Security of Processing”, states the following:

“1. into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

A. the pseudonymisation and encryption of personal data;
B. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
C. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
D. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law" (https://gdpr-info.eu/art-32-gdpr/).

3. AWS encryption policy

AWS also provides a set of guidelines regarding the process, storage and transmission of personal data. When collecting personal data, it is normal for companies to store it in a database, somewhere within the system. However, just because this data is not being used, it doesn't mean it cannot be accessed by threat actors.

This is why data-at-rest should also have strict policies in order to protect it. According to the AWS documentation, "encrypting data at rest is vital for regulatory compliance and data protection. It helps to ensure that sensitive data saved on disks is not readable by any user or application without a valid key" (https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/encrypt-data-at-rest.html).

AWS provides 2 methods to encrypt files and data: disk-level encryption, which provides blockage to an entire disk or part of it using 1 or more keys, and file system-level encryption, that allows to only encrypt specific files without the need to encrypt the entire disk.

AWS also provides services and tools to encrypt data-in-transit, using a file system. "TLS is a set of industry-standard cryptographic protocols used for encrypting information that is exchanged over the network. AES-256 is a 256-bit encryption cipher used for data transmission in TLS. We recommend setting up encryption in transit on every client accessing the file system (https://docs.aws.amazon.com/whitepapers/latest/efs-encrypted-file-systems/encryption-of-data-in-transit.html).

4. GDPR PII requirements

According to the GDPR official website, personal data is understood as any information that can identify a person. If a company has established any kind of process that needs the storage or usage of someone's personal data, this means that it must comply to the GDPR's privacy and security requirements.

GDPR divided the definition of personal data into 4 elements:

- natural person;
- any information;
- inaccurate information;
- identifiable individuals and identifiers.

The GDPR PII requirements can summarized into 10 key requirements:

1. lawful, fair and transparent processing - article 5 demands that all companies should possess documentations regarding the process of storing and collecting personal data;
2. limitation of purpose, data and storage - companies should only collect personal information for specific purposes;
3. data accuracy, integrity and confidentiality - companies should implement technical processes in order to confirm that the data stored is accurate;
4. data protection impact assessment - this is a documentation that provides guidance in proactively identify risks and minimise them;
5. privacy by design - a considerate approach that states that personal data will only be stored during the duration of a project. After its completion, the data will be eliminated;
6. controller-processor contracts - article 28 of the GDPR states that the contracts with the controller and processor should always be compliant with its framework, besides both being clearly identified;
7. data subject rights - provides a list of rights that should be implemented to the personal data subject;
8. data protection officer - an expert that provides guidance with the GDPR requirements and helps companies to maintain and practice them;

9. international data transfers - GDPR is limited to the EU;
10. personal data breach reporting - article 33 requires that the data controller should provide a report within 72 hours for any incident that could reach a high level of risk;

5. GDPR PCI requirements

Payment Card Industry Data Security Standard (PCI DSS) is similar to the PII standards. However, PCI sets guidelines for all companies that collect, storage and use any credit card information of a subject. This is another high level security risk that can provide companies a high number of threats and, possibly, data breaches and stolen data.

There are 12 main requirements set for companies to oblige to them:

1. Install and maintain a firewall configuration for network security to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect cardholder data;
4. Encrypt transmission of cardholder data across open, public networks;
5. Protect all systems against malware and regularly update anti-virus software or programs;
6. Develop and maintain secure systems and applications;
7. Restrict access to cardholder data by business need-to-know;
8. Identify and authenticate access to system components;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes;
12. Maintain a policy that addresses information security for all personnel;